Amendment to the Claims:

Before claim 22, please delete the word "Patent claims" and substitute the following:

What is claimed is:

Please cancel claims 1-21, and add the following new claims:

1-21. (Canceled)

22. (New) A method for operating a security module, said method comprising the steps of:

providing a security module having a secure key memory and at least one data interface;

in a personalization state, setting up a connection to a personalization unit using the data interface;

using the security module to create a module key pair afresh and storing said module key pair in the key memory;

sending a public module key to the personalization unit via the connection;

using the personalization unit to produce a certificate relevant to the public module key by signing with a signing key from the personalization unit;

causing the personalization unit to send the certificate to the security module and storing said certificate securely therein;

clearing down the connection between the security module and the personalization unit; changing the security module from a personalization state to an operating state; and

setting up in the operating state, a cryptographically secure connection to a central system, said connection involving the use of a private module key and involving the public module key together with the certificate being transmitted to the central system, where the certificate is checked.

23. (New) The method as claimed in claim 22, where changeover to the personalization state erases the module key.

24. (New) The method as claimed in claim 22, wherein in the personalization state the connection between the security module and the personalization unit is checked cryptographically for authenticity and is protected against corruption.

25. (New) The method as claimed in claim 22, wherein a public key from the central system is transmitted together with the module certificate, said public key being used in the operating state to check the authenticity of the central system.

26. (New) The method as claimed in claim 25, wherein the public key from the central system is signed with the signing key from the personalization unit, and the resultant certificate is also transmitted and is checked by the security module.

27. (New) The method as claimed in claim 26, wherein a signer's public signing key is signed by the central system creating another certificate, and this certificate is also transmitted and is checked by the security module.

28. (New) The method as claimed in claim 22 wherein the key memory in the security module stores a public checking key from a manufacturer,

the personalization unit transmits its public signing key together with a certificate, formed with the checking key from the manufacturer,

and the security module first checks the public signing key's certificate with the public checking key and then checks the certificates produced with the public signing key,

and changes to the operating state only if the check is successful.

29. (New) The method as claimed in claim 22 wherein the security module is used to form a permanent identity key on a one-off basis, the associated public key is signed with the checking key from a manufacturer, and the corresponding certificate is stored in the security module, and wherein the identity key with a certificate is used to assure the personalization unit of authenticity on the basis of a challenge-response method.

30. (New) The method as claimed in claim 22, wherein the security module sends the personalization module one of a time stamp and a random value which is included in the signature when the certificates are formed.

31. (New) The method as claimed in claim 22, wherein the personalization system sends a variation value to the security module, which is used when the new module key is produced.

32. (New) The method as claimed in claim 22, wherein the connection to the central system which has been set up using the private module key is used to interchange a symmetrical key for subsequent transaction connections and to store it in the secure key memory in the security module.

33. (New) The method as claimed in claim 22, wherein a mobile personalization unit is used which is connected to the security module directly via a connection which is controlled by a user.

34. (New) The method as claimed in claim 22, wherein a user inputs a one-off transaction number into the security module, either directly using an input unit which is connected permanently to the security module or immediately and directly using an input unit which is connected to the security module by the user, and the connection to the personalization unit is protected by transmitting the transaction number.

35. (New) The method as claimed in claim 22, wherein a mobile appliance is connected to the personalization unit via a local connection to the security module, which local connection is controlled directly by a user, and a long-distance connection, the mobile appliance identifies itself to the personalization unit, and as a result the security module is indirectly identified to the personalization unit.

36. (New) The method as claimed in claim 35, wherein the local and long-distance connections are used merely for securely setting up a secure direct network connection between the security module and the personalization unit.

37. (New) A method for personalizing a security module, comprising the following steps:

connecting a security module to a personalization unit;

connecting the security module temporarily to an identification unit the connection being accomplished by a user using an interface which is determined by the user;

sending via the identification unit, an identification value, which can be checked by the personalization unit, to the security module, which forwards it to the personalization unit; and wherein

the personalization unit performs the personalization if the check on the identity value is positive.

38. (New) The method as claimed in claim 37, where the identification value is a one-off transaction number.

39. (New) The method as claimed in claim 38, where the identification value is interchanged between the identification unit and the personalization unit using a cryptographically authenticated data connection.

40. (New) A security module comprising:

a programmable processor including memory for storing a secure key;

at least one data interface for releasably coupling said security module to a personalization unit;

means for creating a module key pair storable in said memory and for sending said module key to said personalization unit;

means for receiving and securely storing a certificate sent from said personalization unit;

operating means for changing said security module from a personalization state to an operating state once said security module is no longer coupled to said personalization unit; and

means for establishing a cryptographically secure connection to a central system using a private module key, said public module key and said certificate.

41. (New) A personalization unit comprising:

at least one data interface for coupling said personalization unit to a security module;

means for receiving a module key via said interface, said module keying being sent from said security module;

means for generating a signing key and producing a certificate regarding said module key, said certificate being produced by signing said module key with said signing key; and

means for sending said certificate to said security module.

42. (New) A central system comprising:

a secure key memory;

at least one data interface;

means for receiving a private module key; a public module key and a certificate from a security module;

means for establishing a cryptographically secure connection to said security module using said public module key, said private module key and said certificate; and

means for checking said certificate.